Essex County College
College Regulation

REG 2-17 COMPUTER AND E-MAIL USAGE

Purpose:

To establish guidelines maintaining the integrity and security of the College's property and information, particularly in light of rapidly growing technology.

Application:

I. By accessing the College's email system, faculty, staff and students assume personal responsibility for its appropriate use and agree to comply with all applicable College codes of conduct, policies and procedures, as well as all applicable local, state, and federal laws and regulations. The individual is solely responsible for access and use of their individual email account and may not share their password or account with anyone.

2. The College has provided computer and communication systems to employees to support the conduct of its business. These systems include individual PCs, mobile devices, and other end-point devices provided to employees, all associated software, the College's telephone, voice mail and electronic mail systems, all centralized computer equipment, and the local and wide-area networks. No use of these systems should ever conflict with the primary business purpose for which they have been provided, with the College's ethical responsibilities or with applicable laws and regulations. Each user is personally responsible to ensure that this Regulation is followed. Access to the College's computer and communications systems is a privilege and must be treated with the highest standard of ethics. All members of the community are expected to use computing and Information Technology Department (IT) resources in a responsible manner.

   Neither the College, nor any office or department thereof, is responsible for:

   (a) the content of e-mail messages that may appear in electronic mailboxes; or

   (b) the use of the information acquired through the College's computing network.

   If user access discloses improper or illegal use, it will be reported and appropriate action taken. Legal processes, including requests for information under the New Jersey Open Public Records Act, may also compel disclosure.

3. All data in the College's computer and communication systems (including print documents, other electronic files, e-mail and recorded voice or video files) is the property of the College. As such, it is subject to disclosure to law enforcement and other third parties. Consequently, employees should always ensure that the business information is securely transmitted via the College's computer and communication systems is accurate, appropriate, ethical and lawful.

4. The College may inspect and monitor such data at any time. No individual should have any expectation of privacy for messages or other data recorded in the College's systems. This includes documents or messages marked "personal and confidential" or "private," which may be inaccessible to most users but remain available to the College. Likewise, the deletion of a document or message may not prevent the College's access to the item or completely eliminate the item from the system.

5. The College strives to maintain a workplace free of harassment and sensitive to the diversity of its employees. The College's systems must not be used to create or transmit material that is derogatory, defamatory, obscene or offensive, such as slurs, epithets, cartoons, images, jokes or anything that might be construed as harassment or disparagement based on race, color, national origin, sex, sexual orientation, gender identity or expression, age, physical or mental disability, medical condition, marital status, religious or political beliefs, or other protected class status. Similarly, the College's systems must not be used to solicit or proselytize others for commercial purposes, causes, outside organizations, chain messages or other non-job-related purposes.

6. Nothing in this policy shall prohibit the use of the College's computer system or Internet access for the purpose of legitimate academic research. However, where such research involves the viewing, copying, downloading or printing of materials which may be considered derogatory, defamatory, obscene or offensive by others, such viewing, copying, downloading or printing of these materials must be performed in a manner which prevents their disclosure to persons who have not knowingly agreed to view their contents.

7. Security procedures in the form of unique user sign-on identification and passwords have been provided to control access to the College's computing system, networks and messaging system. The following activities, which present security risks, should be avoided:

(a) Attempts should not be made to bypass, or render ineffective, security facilities and protocols provided by the College. Security on any computer system is a high priority.

- Faculty, staff, or students who become aware of a security problem should notify the appropriate administrator at once. The user must not demonstrate the problem to other users.

(b) Passwords must never be shared with another individual for any reason.

- If needed, passwords should be managed through a secure password manager. Only the owner of the credentials should have access to the password manager.
- Passwords must never be written down and left in a location easily accessible or visible to others.
- IT will require all passwords to expire on a regular basis. New passwords must be reentered by each user as required.
- In the event a breach or compromise is suspected, the incident must be reported to IT immediately
- Users must notify IT of any changes in the account.

(c) Data with identifiers should not be transmitted.

- Consult with IT prior to transmitting any data with identifiers. Any file transmission of data with user identifiers or any type of confidential College data needs to be authorized by the Area Head and IT. Institutional Effectiveness, Planning and Assessment is exempt from this section 7(c).

(d) Knowingly uploading files that contain malware, or any other similar software or programs that may damage the operation or hardware.

(e) Changes or modifications to the hardware configuration of computer equipment should never be made by individual users. Requests for such changes should be directed to IT.

(f) Additions to, or modifications of, the standard software configuration provided on the College's PCs should never be attempted by individual users.

- Requests for such changes should be directed to IT.

(g) Users must refrain from activities that can compromise the integrity of computing equipment, networks and data.

(h) Expanding access to the network with the addition of personally owned switches, hubs, access points, or other types of network hardware and/or software, and using hardware/software designed to illegally capture network data.

(i) Installation or alteration of wiring, including attempts to create network connections is prohibited.

(j) Scanning of networks, networked devices, or applications for security vulnerabilities without specific authorization by IT is prohibited.

(g) Personal software should never be loaded to the College's computers by individual users. This practice risks the introduction of a computer virus into the system.

- Requests for loading such software should be directed IT.

(h) Downloading information from questionable, unrecognized or unreliable sources.

- Information must be downloaded from trusted, recognized and reliable sources. The failure to download from an appropriate source may subject the College's computer system to viral contamination and/or security breaches.
- Users are expected to demonstrate respect for intellectual property, ownership of data and system security mechanisms.

(i) The College's computer facilities should not be used to attempt unauthorized access to or use of other organizations' computer systems, data or networks.

(j) Computer games should not be loaded on the College's PCs or other end-point devices.

(k) No employee shall remove or copy computer software purchased and licensed by the College from any of the College's computers.

- The College purchases and licenses the use of computer software for business purposes, and does not own the copyright to this software or its related documentation.
- IT, alone, is authorized to install copy and remove software on any of the College's computers.

(l) Unlicensed software should not be loaded or executed on the College's, computer equipment or any other end point devices.

(m) Software documentation for programs developed and/or licensed by the College should not be removed from the College's offices.

(n) The location or installation of computing and telecommunications equipment in offices and work areas should not be changed by individual users.

- Requests for such changes should be directed to IT.

8. There are a number of practices which individual users should adopt that will foster a higher level of security. Among them are the following:

(a) Turn off or lock your computer when you are leaving your work area or office for an extended period of time.

(b) Exercise judgment in storing documents on the College's networks, based on a realistic appraisal of the need for confidentiality or privacy.

(c) Remove and confirm deletion of previously written information from external storage devices before copying documents on such external storage devices for delivery outside the College.

(d) On a frequent and regular basis, back up any information locally stored resource not managed by the College. File sharing of data with user identifiers should only be conducted via a secure and encrypted process approved by IT. Be careful when addressing and sending messages to avoid confidential messages from being delivered to the wrong hands.

(e) Check the message header for accuracy (particularly where people share the same last name and first initial) before sending it. Once sent, a message cannot be stopped from being delivered.

(f) It is the responsibility of the employees and students to protect the confidentiality of their accounts and password information. Users are responsible for all activities associated with their work passwords.

(g) Activities that may strain or compromise College’s e-mail and messaging systems. These activities include but are not limited to sending chain letters, bulk emails, spam, phishing, or any type of unsolicited e-mail.

(h) To prevent security attacks including phishing schemes via email:

- DO NOT click on links or attachments from senders that you do not recognize. Be especially wary of .zip or other compressed or executable file types.
- DO NOT provide sensitive personal information (like usernames and passwords) over email.
- WATCH for email senders that use suspicious or misleading domain names.
- DO NOT respond or reply to spam in any way. Use delete button.
- INSPECT URLs carefully to make sure they’re legitimate and not imposter sites. Malicious websites sometimes use variation in common spelling.
- DO NOT try to open any shared document that you’re not expecting to receive.
- BE CAUTIOUS when opening attachments or clicking links if you receive an email containing a warning banner indicating that it originated from an external source.

9. Any questions about this Regulation should be directed to your Area Head. In an effort to provide you with some guidance, the following is a non-exhaustive list of examples of the common types of conduct which is not acceptable under this Regulation and constitute violations of the Regulation:

(a) Sending, posting, sharing or streaming discriminatory harassing, or threatening messages or images;

(b) Using the College's time and resources for personal gain;

(c) Stealing, using, or disclosing someone else's code or password without authorization;

(d) Violating the copyright law;

(e) Failing to observe licensing agreements;

(f) Engaging in unauthorized transactions that may incur a cost to the College or initiate unwanted internet services and transmissions;

(g) Sending, posting, sharing, or streaming messages or material that could damage the College's image or reputation;

(h) Participating in the viewing or exchange of pornography or obscene materials;

(i) Sending or posting messages that defame or slander other individuals;

(j) Attempting to break into the computer system of another organization or person;

(k) Refusing to cooperate with a security investigation;

(l) Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities;

(m) Using the Internet or College email for political causes or activities, religious activities, or any sort of gambling;

(n) Jeopardizing the security of the College's electronic communication systems;

(o) Sending or posting messages that disparage another College's products or services;

(p) Passing off personal views as representing those of the College;

(q) Sending anonymous electronic messages; and

(r) Engaging in illegal activities.

9. Any employee who violates this Regulation may be subject to disciplinary action up to and including termination, as well as, civil liability and/or criminal sanctions.

Responsible Official(s): Information Technology, Human Resources	**Reference: *N.J.S.A.* 18A: 64A-12(o); *N.J.S.A.* 47:3-8.1 *et seq.,· U.S.C. § 2530 et seq.***
Regulation History: App. 12/99, Rev. 10/01, 7/11, 3/17, 5/23	**Attachment(**s):